UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/027,714
Filing Date: December 21, 2001
Appellant(s): AUSTIN ET AL.

Wesley L. Austin
Reg. No. 42,273
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/10/2006 appealing from the Office action mailed 4/7/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6240530	Togawa	5-2001
6006328	Drake	12-1999

Definition (Type), Dictionary.com, <URL:http://dictionary.reference.com/search?q=type>, retrieved online 3/20/2006

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Togawa U.S. Patent No. 6,240,530, and further in view of Drake U.S. Patent No. 6,006,328.

Togawa teaches a system for the detection and removal of computer malware.

Togawa fails to teach explicitly searching for observer programs as part of that malware.

Drake teaches security methods to protect against attacks by malicious software such as eavesdropping malware.

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the system of Drake with that of Togawa for the advantages of improved security by adding the features of protection against such malicious activities as eavesdropping to the ability of the scanning system as described by Togawa.

It is desirable within any computer system to maintain the security and integrity of such a system while preventing damage to the data and components included therein. Drake teaches protection of the client computer system against malicious software as does Togawa. Although each system teaches protection against a different type of malware by way of scanning the computer system, protecting against all forms of malware is desirable. (Drake Col 3 lines 30-52)

Regarding Claims 1 and 21: Observer program data characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data. (Togawa Fig 1.s1, Col 5 lines 10-19 Drake Fig 4,5 Col 3 lines 31-52) As it is understood the detection of a virus and its type as within Togawa requires recognition of characteristics of a virus. Those characteristics residing within the computer systems various components as any particular virus infects that system; so then the same is true within the combined system for the detection of an observer program as defined by Drake.

Obtain memory data of the computer by using computer instructions (Togawa Fig 1, Col 8 lines 14-30) As explained above the detection of the malware requires checking the system which is inclusive of the memory data; therefore in order for the functionality to proceed it must in some way obtain such data for scanning.

Comparing memory data with observer program data characteristics for detection of an observer program (Togawa Col 8 lines 14-30) As it is known within the art virus scanning is the process of comparing two such sets of data. Further within the

combined system the observer program characteristics are included within the set of the compared traits.

Generating a result of whether an observer program is present (Togawa Fig 1, Fig 3-4 Col 5 lines 10-38) Detection denotes that a result is generated as to the response of the scanning process.

Presenting results through a GUI (Togawa Fig 3-4, Col 5 lines 39-50, Col 13 lines 8-55, Col 14 lines 18-25) As denoted the display performs functions of disseminating operational information which is in a graphical form and presented within an OS that the user is capable of interacting with.

Regarding Claims 2 and 3: Memory data includes startup and registry startup commands (Togawa Col 8 lines 14-30, Col 13 lines 19-56) As stated the memory contains all necessary information for the processes of the machine; these processes being inclusive of starting up necessary portions for operation thereof; such as the OS which includes a registry and the virus detection that being its own implementation scans the memory that these commands are located within.

Regarding Claims 4 and 5: Observer program characteristics include observer import/export table data for comparison with memory import/export table data to determine the presence of an observer program (Togawa Col 8 lines 14-30, Col 13 lines 19-56) As explained above all of the common features of the memory and functionality of the system are scanned via the anti-malware system.

Regarding Claim 6: Observer program characteristics include observer resource data for comparison with memory resource data to determine the presence of an observer program (Togawa Col 8 lines 14-30, Col 13 lines 19-56)

Regarding Claim 7: Observer program characteristics include observer file content data for comparison with memory file content data to determine the presence of an observer program (Togawa Col 8 lines 14-30, Col 13 lines 19-56) Additionally, as is shown and well known within the art file content is compared to malware characteristics for detection of such programs located commonly in such a place.

Regarding Claim 8: The comparing instruction compare the observer file content data with memory file content data at an offset address (Togawa Fig 1, Fig 3-4, Col 5 lines 10-20, Col 13 lines 19-56) The process of scanning for malware is inclusive of the entire range of memory; therefore the process must offset the data being scanned by that which has already been.

Regarding Claim 9: The comparing instruction compare the observer file content data with a span of the memory file content data identified by an offset address (Togawa Fig 1, Fig 3-4, Col 5 lines 10-20, Col 13 lines 19-56) The process of scanning for malware is inclusive of the entire range of memory; therefore that which is scanned is a span of memory that is offset by the amount previously scanned.

Regarding Claim 10: Observer program characteristics include observer module loading data for comparison with memory module loading data to determine the presence of an observer program (Togawa Col 5 lines 10-20, Col 13 lines 19-56)

Regarding Claim 11: Observer program characteristics include OS observing functions for comparison with memory functions from the memory data to determine the presence of an observer program (Togawa Col 5 lines 10-20, Col 13 lines 19-56)

Regarding Claim 12: Memory data includes explorer extension data (Togawa Col 13 lines 19-56)

Regarding Claim 13: Memory data includes file use information (Togawa Col 13 lines 19-56)

Regarding Claim 14: Memory data includes process information (Togawa Col 13 lines 19-56)

Regarding Claim 15: Memory data includes running process information (Togawa Col 13 lines 19-56)

Regarding Claim 16: Memory data includes loaded module information (Togawa Col 13 lines 19-56)

Regarding Claim 17: Memory data includes driver data (Togawa Col 13 lines 19-56)

Regarding Claim 18: Memory data includes kernel driver data (Togawa Col 13 lines 19-56) All of the above stated separate memory data components are included within any resident memory of a common computer system that a system such as the combination of Togawa and Drake would be implemented upon.

Regarding Claims 19 and 20: Instruction to disable an observer program if present (Togawa Fig 1, Fig 10, Col 5 lines 10-50, Col 19 line 15 – Col 20 line 65)

Entering a startup command to load a kill program before the observer program is started (Togawa Fig 10, Col 19 line 15 – Col 20 line 65) As shown within the figure the system clears the memory then loads a secondary extermination routine, inclusive of the secondary OS and associated extermination routine, so that the observer program is not reloaded and instead the kill program is loaded and executed.

Rebooting the computer (Togawa Fig 1, Fig 10) As it is shown after the detection and initial clearing of memory the system must be rebooted with a separate non-infected operating system to further allow for the deletion of any other virus elements.

Starting the kill program by execution of the startup command (Togawa Fig 10, Col 19 line 15 – Col 20 line 65) As explained above the kill program is loaded at startup so the virus may not load.

Deleting the observer program startup command and files (Togawa Fig 10, Col 19 line 15 – Col 20 line 65) The process of clearing the memory as stated within the cited lines and exterminating the malware is the process of deleting the startup command.

(10) Response to Argument

In response to the appellant's argument of the combined reference failing to show "(1) observer data, (2) observer data comprising a plurality of observer program characteristics, (3) observer program characteristics descriptive of a plurality of observer programs, (4) where the observer programs are programmed to observe activities on a computer system and to create log data.", Togawa clearly teaches data that is representative of characteristics of virus programs and when combined with the

teachings of Drake incorporates observer programs into the Togawa system and thus provides for this limitation. Togawa states (Col 5 lines 9-15) "...memory for storing programs and data for information processing and a processing section for executing the programs to perform various information processing, comprising a virus detection and identification section for detecting a computer virus.... and identifying a type of the detected computer virus.." also see Togawa Col 28 lines 31-46. The recitation by Togawa of identifying a type of virus clearly anticipates program characteristics. Type as defined by the American Heritage Dictionary and provided by Dictionary.com is "A number of things having in common traits or characteristics that distinguish them as a group or class", as it can be seen Togawa clearly provides for a manner of identification of types of programs by identifying the characteristics thus providing for recognition of data that consists of a plurality of program characteristics for identifying specific viruses. Additionally, as seen from the recitations of Drake at figure 4, Col 1 lines 55-67, Col 2 lines 18-36, Col 3 lines 6-10, 38-45 while referring to "Rogue Software" (Malware) advantages of detection of these programs is specifically taught by Drake through scanning (Drake Col 4 lines 58-61) of both disks and in memory either at execution or continuously upon certain events. Furthermore, it is an inherent functionality within such a scanning program as noted by Togawa and Drake to provide for the comparison of known characteristics of malware with the data being scanned in order to identify the programs. For further reference see Togawa Col 10 lines 25-67. The systems of both Drake and Togawa perform scanning based upon the characteristics that the Malware imparts upon the system and identifies those Malware by those specific characteristics.

Such characteristics are different for the different programs (Drake Col 1 lines 56-61), whereas the virus itself alters a particular file such other malware has different system altering characteristics such as residing in memory and intercepting system commands (Drake figure 4). As taught by the combination upon scanning and identification of these malicious programs they are then terminated (Togawa Col 10 lines 34-53).

The appellant has argued further that the limitation "...the observer programs are programmed to observe activities on a computer system and to create log data." is not taught by the combined reference. The teachings of Drake within the combination clearly anticipates such observer programs. The appellant states that "rogue software eavesdropping" and "anti-spy techniques" does not teach or suggest observer programs, but from the definition of Drake of rogue software (Drake Col 2 lines 56-67) such programs are clearly anticipated. See Drake abstract, Col 1 lines 45-67, Col 2 lines 1-18, 18-32. Drake recites many different types of observer programs as being rogue software (Col 2 lines 56-67) and further teaches that such programs monitor, steal, and store data of the resident computer as in the case of "keypress password capturers, macro-recorders, and sniffers", thus anticipating observer programs and creating log data.

In response to the appellant's argument of the limitation "comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer." Togawa provides for detection of viruses that are resident within the computer system being scanned, such viruses are logically located in the memory/disks of said computer

system just as in the case of Drake's scanning methods (Drake Col 4 lines 58-61) and the provided scanning program must inherently perform a comparison of memory data and the known program characteristics in order to identify a type and even simply the presence of any malicious program in general. See Togawa Fig 2, 5, 12, 14, Col 10 lines 21-67, Col 16 lines 55-67.

Regarding the appellant's argument of Malware as used within the office action. Togawa clearly teaches the detection of a type of malware (viruses, Trojan horses) (Togawa Col 3 line 46 – Col 4 line 11) and in combination with Drake clearly anticipates all malware (Drake Col 1 lines 45-67, Col 2 lines 1-32) since from the teachings of Drake it is clear that it is a highly desirable effect to be able to provide for protection against all types of "rogue software" (malware) (Drake Col 3 lines 15-45) and such protection cannot be achieved without comprehensive protection against all threats.

The objection presented in the previous action against the drawings requiring a prior art label is withdrawn.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Thomas Szymanski 12/13/2006

Conferees:

Gilberto Barron

Matthew Smithers

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100